DIGITAL DATA FILE ENCRYPTION APPARATUS AND METHOD AND RECORDING MEDIUM FOR RECORDING DIGITAL DATA FILE ENCRYPTION PROGRAM THEREON

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to digital data file encryption in which an encrypted digital data file is prevented from illicit interception and decoding when digital audio data or digital video data is transmitted to a personal computer through a computer communication network and, in turn, downloaded to a digital data player such as an MP3 player.

2. Description of the Related Art

MP3 (shorthand for MPEG-1 Layer 3 Audio) is one of various available digital data formats for audio data. An MP3 player is a new notional, portable digital device capable of readily downloading and reproducing desired data from a computer communication network using an audio data compression coding technique prescribed in MPEG-1 Layer 3. The MP3 player has few faults and excellent sound quality because it stores a file in the form of digital data. Further, the MP3 player is small in size and light in weight, thereby assuring high portability such that a user can carry it even during his physical exercise. For these reasons, this product is a viable alternative to a portable cassette tape recorder and compact disk (CD) player.

With reference to Fig. 1, there is shown in block form a conventional arrangement of a digital data player and associated peripheral devices. In this drawing, the reference numeral 10 denotes a digital data server which assigns an identification (ID) number and password (PWD) to a personal computer 20 for user registration, and which also transmits a digital data player 22 in software form to the personal computer 20. Upon receiving a file supply request from the user, the digital data server 10 identifies the user on the basis of an ID number and password entered by him and supplies an encrypted digital data file to the user in accordance with this identification.

The personal computer 20 stores the digital data file supplied from the digital data server 10 on a hard disk 21 therein and decrypts it through the downloaded software player 22 to reproduce the resultant unencrypted digital data file or to download it to a digital data playing device 30. The digital data playing device 30 downloads the unencrypted data file from the personal computer 20 and stores it in a memory unit 40 for the reproduction thereof. The memory unit 40 downloads the unencrypted digital data file from the digital data playing device 30 and stores it in its internal memory 42 to output the file for a desired playing operation.

The operation of the conventional arrangement with the above-mentioned construction will now be described.

In order to legally receive a desired digital data file from the digital data server 10, the user has to register with a digital data file supplier. During user registration, the user is assigned an ID number and password from the digital data file supplier. Then, the user downloads a digital data player 22 in software form from the digital data server 10 through a communication network and installs the downloaded digital data player 22 in the personal computer 20.

Thereafter, to download a desired digital data file from the digital data server 10 through the personal computer 20 and communication network, the user transmits his ID number and password to the digital data server 10 through the personal computer 20 and communication network. The digital data server 10 identifies the user on the basis of the transmitted ID number and password and supplies the desired digital data file to the user in accordance with the identification. At this time, the digital data server 10 encrypts the digital data file using the user's ID number as an encryption key and transmits the encrypted digital data file to the personal computer 20.

The personal computer 20 stores the digital data file transmitted from the digital data server 10 on the hard disk 21. Then, upon receiving a reproduction request from the user, the personal computer 20 decrypts and reproduces the stored digital data file via the digital data software player 22. As a result, the user is able to listen to desired music through the personal computer 20.

On the other hand, if the user intends to listen to music in a digital data file form using the portable digital data playing device 30, then the personal computer 20 decrypts the digital data file, stored on the hard disk 21 with the digital data software player 22,

and sends the decrypted digital data file to the digital data playing device 30 through a download unit 23 therein and the communication network.

Then, the digital data playing device 30 stores the digital data file, sent along the above path, in the memory 42 of the memory unit 40, which is typically in the form of a removable card. If the user requests the digital data player 30 to reproduce the digital data file stored in the memory 42, then the digital data player 30 reads the stored digital data file from the memory 42 and reproduces it through a decoder 32 therein. As a result, the user can listen to desired music anywhere using the digital data player 30.

However, the above-mentioned conventional arrangement has a disadvantage in that the digital data file may be intercepted from the communication network during downloading from the personal computer to the digital data playing device (or from the digital data playing device to the memory card) in an unencrypted condition. Such an interception of the unencrypted digital data file makes it impossible to protect the copyright of a music copyright holder and music copyright associates (for example, a music producer and planner taking charge of music production, duplication and distribution). In order to solve the above problem, a conventional powerful encryption method may be used to powerfully encrypt the digital data file and send it to the digital data player. However, such powerful encryption, in turn, requires a powerful decryption function, thereby increasing the cost of the digital data player.

SUMMARY OF THE INVENTION

Therefore, the present invention has been made in view of the above problems, and it is an object of the present invention to provide an encryption system in which illegal outflow of a digital data file, such as MP3, downloaded from a server can be prevented, with no additional increase in cost.

In accordance with one aspect of the present invention, there is provided a method for encrypting digital data including decrypting digital data which has been encrypted at a high encryption level, storing a predetermined amount of the decrypted digital data in a buffer, reencrypting output digital data from the buffer at a low encryption level; and transferring the reencrypted digital data to a digital data player or a data storage medium.

In accordance with another aspect of the present invention, there is provided a

method for encrypting digital data including determining whether digital data which has been encrypted at a high encryption level must be protected from unauthorized copying, decrypting the digital data, transferring the decrypted digital data to a digital data player or a data storage medium if the decrypted digital data need not be protected from unauthorized copying, and reencrypting the decrypted digital data at a low encryption level if the decrypted digital data must be protected from unauthorized copying.

In accordance with a further aspect of the present invention, there is provided a program (or script) embodied on a computer-readable medium for encrypting or decrypting a digital data file, the computer-readable-medium-embodied program including a first program code segment to receive and store digital data encrypted to a high level and an encryption key, a second program code segment to decrypt the stored digital data using the encryption key, a third program code segment to store a predetermined amount of the decrypted digital data in a buffer, and a fourth program code segment to reencrypt the digital data from the buffer to a low level and download the reencrypted digital data to a digital data player or a data storage medium.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other objects, features and advantages of the present invention will be more clearly understood from the following detailed description taken in conjunction with the accompanying drawings, in which:

Fig. 1 is a block diagram of a conventional arrangement of a digital data player and the associated peripheral devices

Fig. 2 is a block diagram of an embodiment of a digital data file encryption apparatus in accordance with the present invention;

Figs. 3A to 3E are views illustrating examples of file encryption in accordance with the present invention;

Fig. 4 is a flowchart illustrating a digital data file encryption method in accordance with the present invention; and

Fig. 5 is a block diagram of an alternative embodiment of the digital data file encryption apparatus in accordance with the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

With reference to Fig. 2, there is shown in block form an embodiment of a digital data file encryption system in accordance with the present invention. The operation of the digital data file encryption system according to the present invention will hereinafter be described in detail with reference to Figs. 2 to 4.

First, the user must register with a digital data file supplier to legally receive a desired digital data file from a digital data server 110. During user registration, the user is assigned an ID number and password from the digital data file supplier. Then, the user downloads a digital data player 122 in a software form from the digital data server 110 through a communication network and sets the downloaded digital data player 122 in a personal computer 120.

Thereafter, the user transmits his ID number and password to the digital data server 110 through the personal computer 120 and communication network to download a desired digital data file from the digital data server 110 through the communication network. The digital data server 110 identifies the user on the basis of the transmitted ID number and password and supplies the desired digital data file to the user in accordance with the identification. At this time, the digital data server 110 encrypts the digital data file on the basis of a predetermined encryption key and transmits the encrypted digital data file to the personal computer 120.

The personal computer 120 stores the digital data file transmitted from the digital data server 110 on a hard disk 121 therein. Then, upon receiving a reproduction request from the user, the personal computer 120 decrypts and reproduces the stored digital data file through the digital data software player 122. As a result, the user can listen to desired music through the personal computer 120.

On the other hand, in the case where the user intends to listen to music in a digital data file form using a digital data playing device 130, the personal computer 120 has to transmit the desired digital data file to the digital data playing device 130. In this case, if the digital data file is powerfully encrypted and downloaded to the digital data playing device 130, a corresponding powerful decryption function must be performed in the digital data playing device 130. Such powerful decryption would result in an increase in cost of the digital data playing device 130. Alternatively, when the digital data is downloaded under the decrypted, or non-processed, condition, it is subject to

illicit diversion during transmission, and subsequent uncontrolled distribution. In order to overcome the above problems, the present encryption apparatus encrypts and downloads the digital data file in the following manner.

In the personal computer 120, an encrypted data file from the hard disk 121 is decrypted by an encryption decryptor 123, temporarily stored in a buffer 124, and then transferred to an encryption/download unit 125. Noticeably, different types of data files may be transferred to the encryption/download unit 125 along the same path. At this time, it is determined whether a given data file must be protected during transmission because of a copyright. If the given data file is determined to be copyrighted, then the buffer 124 is appropriately changed in size according to the size (capacity) of the given file. To the contrary, in the case where the given data file need not be protected because of a copyright, then it is directly downloaded to the digital data playing device 130.

Changing the size of the buffer 124 appropriately as needed causes the decrypted data not to be normally used even if it is hacked or illicitly diverted while being stored in the buffer 124. By way of illustration, if the effective size of the buffer is large, a relatively long time is needed to encrypt the decrypted data in the memory. In such a case, a hacking program can find a position of the decrypted data in the memory and illicitly divert such data. Thus, the buffer size according to the present invention is advantageously made small, thereby reducing the amount of time decrypted data remains in the buffer and is susceptible to diversion.

However, as a practical matter, if the buffer size becomes too small, there will be unnecessary time spent making many transfers of data from a hard disk to the buffer, and data transfer speed will be reduced. Thus, in order to maintain an appropriate data transfer rate, the buffer size is set at, for example, one of some fraction (e.g., 1/1000) of the data file size, or some set length of processing time of a conventional personal computer (e.g., 0.1 seconds of a 233 MHz processor). The buffer size may be set to the smaller of the above two values, or the larger of the values, depending on system design considerations. As a result of this small buffer size, the hacking or illicit diversion of the data file so protected does not frustrate the purposes of copyright laws, because the diverted file cannot be used.

For example, assume that a digital data file to be protected in copyright has a three-minute capacity and it is normally reproducible only when being stored in the

buffer 124 in the unit of two-second amounts. In this case, the one-second amount-unit storage of the digital data file in the buffer 124 causes the digital data file not to be normally used even when it illegally flows. As a result, the copyright of the digital data file can be protected. There may be various methods for identifying files to be protected in copyright. One such method is to identify files to be protected in copyright on the basis of extension indexes.

In the case where the output digital data from the buffer 124 need not be protected in copyright, it is downloaded directly in unencrypted form to the digital data playing device 130 through the encryption/download unit 125. However, if the copyright of the output digital data from the buffer 124 must be protected, then the file is weakly encrypted and downloaded to the digital data playing device 130 by the encryption/download unit 125.

Figs. 3A to 3E are views illustrating examples of file encryption in accordance with the present invention. For weak encryption, a strongly encrypted file as shown in Fig. 3A is partially decrypted on the basis of a predetermined encryption key and the remaining parts thereof are left strongly encrypted. As a result, a file encrypted and downloaded by the encryption/download unit 125 has striped, strongly encrypted areas as shown in Fig. 3B. Here shading denotes encrypted data and no shading denotes unencrypted data.

Alternatively, the file encrypted as shown in Fig. 3A may be totally decrypted as shown in Fig. 3C and then more weakly encrypted/downloaded as shown in Fig. 3D on the basis of the predetermined encryption key. Alternatively, the unencrypted file shown in Fig. 3C may have only portions weakly encrypted as shown in Fig. 3E. Any of the encryption schemes shown in Figs. 3B, 3D, or 3E reduce processing requirements for the digital data playing device 130 relative to a file where all of the data has been strongly encrypted.

The digital data playing device 130 stores the digital data file from the personal computer 120, encrypted and downloaded in the above manner, in a memory 142 of a data storage medium 140 which may be in the form of a removable card. If the user requests the digital data playing device 130 to reproduce the digital data file stored in the memory 142, then the digital data playing device 130 reads the stored digital data file from the memory 142 and reproduces it through a decoder 132 therein. At this time, the

digital data file read from the data storage medium 140 has to be decrypted for the reproduction because it is in an encrypted form. For this reason, in the digital data playing device 130, a microcomputer 131 decrypts the digital data file read from the data storage medium 140 on the basis of the encryption key used in the above encryption procedure and outputs the decrypted digital data file to an output line through the decoder 132. Because of the weak encryption shown, for example, in Figs. 3B, 3D, and 3E, the decoder is kept low-cost. As a result, the user can listen to desired music anywhere using the digital data playing device 130 and the digital data file can be prevented from illicit diversion and distribution while being downloaded to the digital data playing device 130.

In accordance with the present invention, the above encryption method may be implemented by one program on a recording medium. The encryption program is configured to receive and store both digital data encrypted to a high level and an encryption key, decrypt the encrypted digital data according to the encryption key, store the decrypted digital data in a buffer in a predetermined unit of size, reencrypt output digital data from the buffer to a low level and download the reencrypted digital data to a digital data player or a data storage medium. This encryption program is stored on a single recording medium for use in the digital data encryption of the present invention.

Fig. 4 is a flowchart illustrating a digital data file encryption method in accordance with the present invention. First, upon receiving a digital data file download request from a personal computer at step 410, a server identifies the user at step 420 to determine whether the user is legitimate. At this time, the server identifies the user on the basis of an ID code and password which are assigned from the server to the user, as stated previously. If the user is identified to be legitimate, the server downloads a desired digital data file encrypted to a high level and an encryption key to the personal computer at step 430. Upon downloading the desired digital data file from the server, the personal computer determines at step 440 whether a copyright of the downloaded file must be protected. If the downloaded digital data file need not be protected in copyright, then it is decrypted and downloaded directly to a digital data player at step 510. In this case, because no copyright problem is caused even when the downloaded file is hacked/diverted, there is no necessity for encrypting the downloaded file to send it to the digital data player.

On the other hand, in the case where it is determined at the above step 440 that the copyright of the downloaded file must be protected, the personal computer first checks the capacity of the downloaded file at step 450 and then sets an effective capacity of a buffer in accordance with the checked result at step 460. Then, the personal computer decrypts the downloaded file according to the encryption key at step 470 and stores the decrypted file in the buffer at step 480 in such a manner that the decrypted file cannot be normally reproduced even when it is hacked in process of being downloaded to the digital data player. The digital data file stored in the buffer is encrypted to a low level at step 490. This low level encryption does not require a separate microprocessor which is typically used for the high level encryption or powerful encryption, thereby avoiding an increase in cost of the associated playing device. Then, the digital data file encrypted to the low level is downloaded to the digital data playing device at step 500.

With reference to Fig. 5, there is shown in block form an alternative embodiment of the digital data file encryption system in accordance with the present invention. This second embodiment is substantially the same in construction as the first embodiment, with the exception that a plurality of digital data servers 110A-110C are provided. Because of the provision of the plurality of digital data servers, the personal computer 20 performs the decryption operation, not using the single encryption key as shown in Fig. 2, but using a plurality of encryption keys supplied respectively from the digital data servers. Then, the personal computer 20 reproduces the decrypted, or non-processed, digital data files or downloads them (with or without encryption) to the digital data playing device 130 in the same manner as stated previously.

According to the present invention, a digital data file downloaded from a single server is decrypted, stored in the buffer in a predetermined unit of size, encrypted in a somewhat simple manner and downloaded to the digital data player. Digital data files downloaded from a plurality of servers are decrypted in individual decryption manners, encrypted in the simple manner as mentioned above and downloaded to the digital data player. Therefore, it is possible to reliably protect the copyright of a given digital data file without increasing the cost of the digital data player due to the decryption function.

Although the preferred embodiments of the present invention have been disclosed for illustrative purposes, those skilled in the art will appreciate that various modifications, additions and substitutions are possible, without departing from the scope

and spirit of the invention as disclosed in the accompanying claims.

0607650 - 052705